法国的一家医疗保险公司借助 IBM Security 改善了安全态势、事件响应及运营效率

客户情况：

- 作为一家医疗保险公司，该客户非常重视数据安全与机密性。该公司需要为其客户处理必须确保安全的各种敏感数据。因此，该公司必须要确保以妥当的方式处理所有敏感数据，同时确保这些数据的使用不会违反行业监管法规及公司的合约条款规定。为此，该公司希望找到一款安全解决方案，可帮助他们确保高效的数据管理和使用、维持监管合规性并维持客户对公司的信心。

IBM 解决方案：

- 该公司一直使用的是 IBM Security 的解决方案套件，包括 IBM Security QRadar、IBM Resilient 及 IBM Security QFlow 软件，以满足其数据安全需求。该公司决定迁移到最新一代的 IBM Security 解决方案软件，以满足不断变化并增长的需求。
- 该客户安装了 IBM QRadar Network Insights V1901 软件，替换了之前安装的 QFlow 1202，前者可为其提供更准确的威胁检测和预测功能。该客户还升级到了 IBM Security QRadar SIEM XX29 软件，替换了之前使用的 IBM Security QRadar SIEM XX05 解决方案。Security QRadar SIEM 解决方案作为数据安全平台的基础，通过实时分析为该客户提供了更准确的威胁检测及优先排序功能。最后，该客户从物理形式的 Resilient 软件解决方案迁移到了软件即服务 (SaaS) 解决方案。该客户在其安全运营中心采用了 Resilient SaaS 解决方案，用以管理事件响应。

客户收益：

- 借助升级的解决方案，安全平台比之前更为灵活、服务水平更高，不仅节省了大量成本，也能够更好地满足不断变化的需求。借助这些解决方案，该公司的整体 IT 安全管理与事件响应水平也得到了改善。此外，该公司的所有利益相关者均可访问运营解决方案，不仅提升了运营效率，还进一步提升了整体安全性。

客户资料：

该公司成立于 2013 年，是法国的一家医疗保险公司。该公司的总部位于法国巴黎，拥有 2,000 多名员工，在全国范围内建立了庞大的运营网络，包括 20,852 家分公司及 200 多个办事处。该客户致力于为法国超过 130 万名客户提供服务。

IBM Security 帮助英国的一家全球银行优化了安全监控流程，提升了网络威胁检测和响应能力

客户情况：

- 过去，该客户一直依赖分散、脱节的威胁检测平台来应对 **12 个孤立的安全运营中心 (SOC)**，监控信息和安全风险。结果，该银行在洞悉各个实体内的威胁时，只能获得**支离破碎的可视性**。更糟糕的是，SOC 每天只工作八小时，一周只工作五天，导致客户一周有很长一段时间处于无人监管的状态。此外，该银行**依靠数名全职员工来运营 SOC 和提供合规性报告**。因此，银行的运营成本非常高。为了解决这些问题，客户希望利用一款强大的安全解决方案来**实现 SOC 的转型**。

IBM 解决方案：

该客户分三个阶段实施 IBM 安全软件，构建集成式 SOC。

1. 在第 1 阶段，客户制定了端到端的 SOC 转型路线图。他们**开展了成熟度评估**，编制了 SOC 章程，制定了投资计划。然后，为了实现 SOC 的转型，客户实施了 IBM Security QRadar SIEM 软件来准确检测客户面临的威胁，并对威胁进行优先级排序。
2. 在第 2 阶段，该银行**将 Security QRadar SIEM 软件推广至其余的 11 个本地 SOC**，以改进智能威胁检测和响应。借此，客户消除了平台孤岛，将 SOC 集成到了**全天 24 小时运行**的连贯系统中。
3. 在第 3 阶段，为了增强 SOC 功能，客户部署了 IBM Resilient Incident Response Platform，以便**自动执行 SOC 工作流管理和事件响应流程。**

客户收益：

- 通过实施上述解决方案，该客户能够通过单一界面**获得**覆盖整个企业的**可视性**，**更高效**地检测和响应网络威胁，**降低事件的影响，不再需要全职员工**来持续监控系统，进而大幅**减少运营成本**。

客户资料：

该公司是一家总部位于英国的大型全球银行。